



MaxKB: RCE via MCP stdio command injection in workflow engine

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-39417
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 00:16:07 UTC
Updated	2026-04-14 00:16:07 UTC
Description	MaxKB is an open-source AI assistant for enterprise. Versions 2.7.1 and below contain an incomplete fix for CVE-2025-539

Risk And Classification

Primary CVSS: v3.1 4.6 MEDIUM from security-advisories@github.com

CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L

Problem Types: CWE-20 | CWE-78 | CWE-78 CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | CWE-20 CWE-20: Improper Input Validation

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	4.6	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	4.6	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	1Panel-dev	MaxKB	affected < 2.8.0	Not specified

References

Reference	Source	Link
github.com/1Panel-dev/MaxKB/commit/50e96002ee5dca34c68d3d9333b64ea358c92304	security-advisories@github.com	github.com
github.com/1Panel-dev/MaxKB/releases/tag/v2.8.0	security-advisories@github.com	github.com
github.com/1Panel-dev/MaxKB/security/advisories/GHSA-pw52-326g-r5xj	security-advisories@github.com	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)